PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G06K 7/00 — A1

(11) Internationale Veröffentlichungsnummer: **WO 00/63827**

(43) Internationales Veröffentlichungsdatum: 26. Oktober 2000 (26.10.00)

(21) Internationales Aktenzeichen: PCT/EP00/03429

(22) Internationales Anmeldedatum: 14. April 2000 (14.04.00)

(30) Prioritätsdaten:
99107578.9 15. April 1999 (15.04.99) EP

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Str. 53, D-81541 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: WEDER, Uwe [DE/DE]; Im Bäckerfeld 23 A, D-84072 Au/Hallertau (DE).

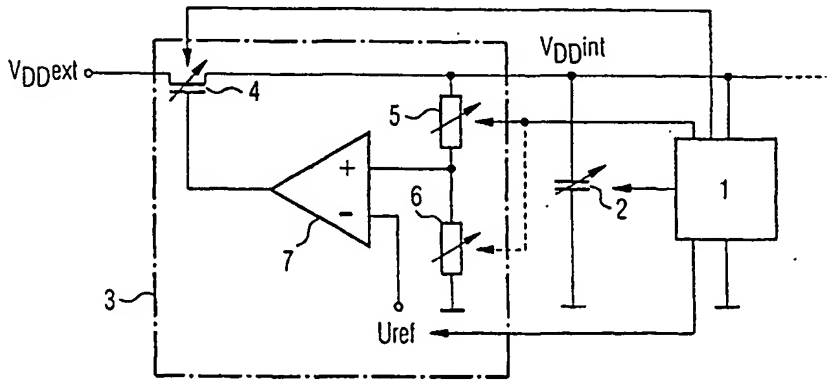
(74) Gemeinsamer Vertreter: INFINEON TECHNOLOGIES AG; Zedlitz, Peter, Postfach 22 13 17, D-80503 München (DE).

(81) Bestimmungsstaaten: BR, CN, IN, JP, KR, MX, RU, UA, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: INTEGRATED CIRCUIT WITH A CONTROLLABLE VOLTAGE REGULATOR

(54) Bezeichnung: INTEGRIERTE SCHALTUNG MIT STEUERBAREM SPANNUNGSREGLER



(57) Abstract

Disclosed is a circuit integrated on a semiconductor-chip. The aim of the invention is to hide the current profile which can be detected on the input terminal of the supply voltage. To this end, the characteristics of a voltage regulator can be changed.

(57) Zusammenfassung

Es wird eine auf einem Halbleiter-Chip integrierte Schaltung beschrieben, bei der eine Verschleierung des an einer Versorgungsspannungseingangsklemme detektierbaren Stromprofils durch einen in seinen Eigenschaften änderbaren Spannungsregler erreicht wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Integrierte Schaltung mit steuerbarem Spannungsregler

Integrierte Schaltungen insbesondere solche zur Verwendung in tragbaren Datenträgern wie Chipkarten bieten viele Manipulations- und/oder Analyseanreize, da sie zunehmend in sicherheitskritischen Bereichen wie Zutrittskontrolle, als wiederaufladbare Geldkarte oder zur Erzeugung elektronischer Unterschriften eingesetzt werden.

Die für die Sicherheit der genannten Anwendungen maßgeblichen Elemente sind zumeist speziell konfigurierte Schaltungsteile oder in nicht-flüchtigen Speichern abgelegte geheime Informationen. Um ein Ausspähen dieser Details zu verhindern wurde in der Vergangenheit vorgeschlagen, Schaltungsteile in tieferen Ebenen der integrierten Schaltung zu realisieren, so daß durch darüberliegende Strukturen verdeckt sind. Andere Vorschläge zielten auf eine zusätzliche vorzugsweise leitende Abdeckung der integrierten Schaltung, die in die Stromversorgung einbezogen ist und deren Vorhandensein bzw. Unversehrtheit detektiert werden kann, um den Verarbeitungsablauf in der integrierten Schaltung entsprechend zu beeinflussen. Darüberhinaus ist auch schon eine Verschlüsselung des Datenaustauschs zwischen Bestandteilen einer Schaltung auf einem einzigen Halbleiterchip vorgeschlagen worden.

All diese Schutzmaßnahmen greifen jedoch nicht in ausreichendem Maße bei einer seit einiger Zeit bekanntgewordenen Analysemethode, die sich auf die Beobachtung und statistische Auswertung des von außen meßbaren Strukturprofils bei bestimmungsgemäßem Gebrauch beschränkt, ohne also den Halbleiterchip zu verändern. Diese Methode ist unter der englischen Bezeichnung Differential Power Analysis bekannt geworden und eine kurze Beschreibung dieser Methode ist beispielsweise in der Internet-Seite http://www.cryptography.com veröffentlicht.

Danach hat es sich gezeigt, daß bei gleichen Abläufen innerhalb der integrierten Schaltung - beispielsweise bei Ausführung des gleichen Befehls in einem Mikroprozessor - das gleiche Stromprofil an der Versorgungsspannungseingangsklemme meßbar ist. Durch statistische Auswertung dieses Stromprofils können sogar einzelne Bits einer für eine Verschlüsselung erforderlichen geheimen Zahl ermittelt werden.

Die Aufgabe vorliegender Erfindung ist es, einen Schutz vor einer solchen Analyse zu bieten.

Die Aufgabe wird durch eine auf einem Halbleiterchip integrierte Schaltung mit dem Merkmal des Anspruchs 1 gelöst. Vorteilhafte Weiterbildungen sind in den Unteransprüchen angegeben.

Die erfindungsgemäße integrierte Schaltung weist also einen Versorgungsspannungsregler auf, der prinzipiell die Spannung an einem Ladungsspeicher, insbesondere einem Pufferkondensator, stabilisieren soll. Der Ladungsspeicher kann aber auch bereits durch die Kapazität der integrierten Schaltung selbst gegeben sein. Dieser Spannungsregler arbeitet aber nicht konstant auf einem Arbeitspunkt sondern wird durch eine Steuereinheit in seinen Regeleigenschaften verändert. Hierdurch werden die durch den Datenverarbeitungsteil der integrierten Schaltung erzeugten Stromprofilschwankungen durch die vom Spannungsregler stammenden Schwankungen überlagert, so daß das tatsächliche Stromprofil verschleiert wird und somit bei gleichen Verarbeitungsvorgängen innerhalb der integrierten Schaltung aufgrund der Änderungen der Parameter der Regelschaltung unterschiedliche Stromprofile resultieren und somit kein Zusammenhang zwischen Stromprofil und Verarbeitungsvorgang mit statistischen Methoden hergeleitet werden kann.

In einer Variante der Erfindung wird statt oder zusätzlich zu dem Spannungsregler die Kapazität des Ladungsspeichers geän-

dert. Dies entspricht in seiner Auswirkung dem Ändern des Widerstands eines Längsregeltransistors bei einem Serienregler, da hierdurch die Zeitkonstante des durch diesen Längsregeltransistor und den Ladungsspeicher gebildeten Tiefpasses beeinflußt wird.

Um eine erfolgreiche Beeinflussung des Stromprofils zu erzielen müssen die Änderungen der Regler- bzw. Ladungsspeichereigenschaften zeitlich und hinsichtlich der Auswirkung auf die Amplitude des Stromprofils im Bereich der typischen Werte der durch schaltungsinterne Vorgänge hervorgerufenen Änderungen liegen.

Besonders vorteilhaft wirkt sich eine Änderung der internen Versorgungsspannung zu niedrigeren Werten hin aus, die in diesem Fall auch langsamer sein kann, da dann bei besonders sicherheitskritischen Vorgängen die Energie allein aus dem Ladungsspeicher bezogen werden kann, ohne daß dies im Ladestrom zu einer Profilierung führen würde. Eine Nachladung des Ladungsspeichers kann bei nicht-sicherheitskritischen Vorgängen erfolgen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe einer Figur näher erläutert.

Die Figur zeigt eine integrierte Schaltung gemäß der Erfindung, die ein Teil einer auf einem Halbleiterchip realisierten Schaltung ist. Der nicht zur Erfindung gehörende Teil der gesamten integrierten Schaltung, die durch die interne Versorgungsspannung $V_{DD}int$ versorgt wird ist durch eine gepunktete Fortsetzung der Versorgungsspannungsleitung dargestellt.

Zwischen der Klemme, an die die externe Versorgungsspannung $V_{DD}ext$ angelegt wird und dem einen Anschluß eines als Pufferkondensator 2 ausgebildeten Ladungsspeichers ist im gewählten Ausführungsbeispiel der Längsregeltransistor 4 eines Serienspannungsreglers 3 geschaltet. Dieser wird von einem Regel-

verstärker 7 angesteuert. Die beiden Eingänge des Regelverstärkers 7 sind einerseits mit einer Referenzspannung Uref und andererseits mit dem Mittelabgriff eines als Ist-Spannungsmeßeinrichtung fungierenden Spannungsteilers 5, 6 verbunden. Der Spannungsteiler 5, 6 ist parallel zum Pufferkondensator 2 geschaltet. Durch diese Schaltung soll zunächst erreicht werden, daß die interne Versorgungsspannung $V_{DD}int$ auf einem durch die Referenzspannung Uref definierten Wert gehalten wird.

In erfindungsgemäßer Weise sind nun sowohl der als Stellglied des Spannungsreglers fungierende Längsregeltansistor 4, die Widerstände des Spannungsteiler 5, 6, der Pufferkondensator 2 und auch die Referenzsspannung Uref änderbar ausgebildet, was durch Pfeile angedeutet ist, und können von einer Steuerschaltung 1 angesteuert werden. Die Änderbarkeit kann zum Beispiel durch Parallelschaltung zusätzlicher entsprechender Bauteile erreicht werden. Dabei genügt es prinzipiell, wenn nur eines der genannten Elemente änderbar ausgebildet ist beziehungsweise angesteuert wird. Um aber im Sinne der zu lösenden Aufgabe eine Verschleierung des tatsächlichen Stromprofils an der Eingangsklemme ($V_{DD}ext$) zu erreichen, ist es von Vorteil, wenn mehrere Möglichkeiten vorhanden sind, die abwechselnd oder auch zusammen eingesetzt werden können.

Die durch die Steuereinheit 1 gesteuerten Änderungen können dabei langsam sein, um zum Beispiel für bestimmte Operationen durch Verändern der Referenzspannung Uref oder des Spannungsteilers 5, 6 die interne Versorgungsspannung $V_{DD}int$ abzusenken, so daß die Versorgung des (nicht dargestellten) Datenverarbeitungsteils der integrierten Schaltung allein aus dem Pufferkondensator 2 erfolgen kann. Dies ist bei sicherheitskritischen Datenverarbeitungsvorgängen wie beispielsweise Verschlüsselung von Interesse, da dann kein spezifisches Stromprofil an den Eingangsklemmen detektierbar ist.

Andererseits können auch schnelle, zufällige Veränderungen, die sich im Pegel- und Frequenzbereich der typischen Stromprofilschwankungen bewegen sinnvoll sein, um auf diese Weise der Überlagerung der tatsächlichen Schwankungen mit den aufgezwungenen eine Verschleierung zu erreichen, die eine statistische Auswertung erschwert oder gar verunmöglicht.

Ein besonderer Vorteil der erfindungsgemäßen integrierten Schaltung besteht darin, daß die Stromverschleierung nicht auf Kosten eines zusätzlichen Leistungsverbrauchs geht.

Patentansprüche

1. Auf einem Halbleiterchip integrierte Schaltung
mit einer Steuereinheit (1),
mit einem internen Ladungsspeicher (2), an dem die interne Versorgungsspannung (V_{DD}int) der integrierten Schaltung abgreifbar ist,
mit einer externen Versorgungsspannungsklemme zur Versorgung der integrierten Schaltung mit einer externen Versorgungsspannung (V_{DD}ext),
mit einem zwischen der externen Versorgungsspannungsklemme und dem Ladungsspeicher (2) angeordneten Spannungsregler (3),
wobei der Spannungsregler (3) und/oder der Ladungsspeicher (2) mit der Steuereinheit (1) derart verbunden ist, daß Betriebsparameter des Spannungsreglers (3) und/oder des Ladungsspeichers (2) durch ein Steuersignal der Steuereinheit (1) änderbar ist bzw. sind.

2. Integrierte Schaltung nach Anspruch 1, **dadurch gekennzeichnet**, daß das Stellglied (4) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.

3. Integrierte Schaltung nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die Meßeinrichtung (5, 6) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.

4. Integrierte Schaltung nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß der Sollwert (Uref) des Spannungsreglers (3) durch das Steuersignal ansteuerbar ist.

5. Integrierte Schaltung nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, daß das Steuersignal ein Zufallssignal ist.

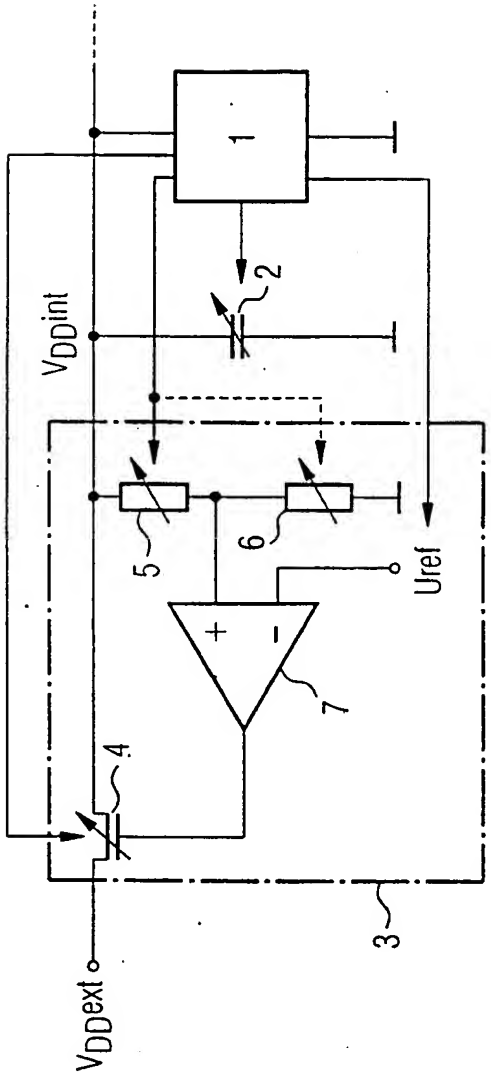


Fig 1

INTERNATIONAL SEARCH REPORT

Inte. onal Application No
PCT/EP 00/03429

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 479 172 A (SMITH GREGORY M ET AL) 26 December 1995 (1995-12-26)	1-4
A	column 4, line 62 -column 11, line 17; figures 1-11	5
A	EP 0 568 398 A (GEC AVERY LTD) 3 November 1993 (1993-11-03) the whole document	1-5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2000	06/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte onal Application No
PCT/EP 00/03429

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5479172 A	26-12-1995	NONE	
EP 0568398 A	03-11-1993	GB 2266794 A	10-11-1993

INTERNATIONALER RECHERCHENBERICHT

Inte onales Aktenzeichen
PCT/EP 00/03429

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06K7/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 479 172 A (SMITH GREGORY M ET AL) 26. Dezember 1995 (1995-12-26)	1-4
A	Spalte 4, Zeile 62 -Spalte 11, Zeile 17; Abbildungen 1-11	5
A	EP 0 568 398 A (GEC AVERY LTD) 3. November 1993 (1993-11-03) das ganze Dokument	1-5

[ ] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. Juni 2000	06/07/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/03429

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5479172 A	26-12-1995	KEINE	
EP 0568398 A	03-11-1993	GB 2266794 A	10-11-1993